



# 642-648<sup>Q&As</sup>

Deploying Cisco ASA VPN Solutions (VPN v2.0)

## Pass Cisco 642-648 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/642-648.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

Which statement is true about configuring the Cisco ASA for Active/Standby failover?

- A. All versions of Cisco ASA software need to have the same licensing on both devices.
- B. Both devices perform load sharing until a failure occurs.
- C. All VPN-related configurations and files are automatically replicated.
- D. VPN images, profiles, and plug-ins must be manually provisioned to both devices.

Correct Answer: D

### QUESTION 2

Refer to following Exhibit and answer the following question below: The user, contractor1, will receive an IP address when the VPN connection is established. Which statement regarding the IP address is true?

**Instructions**

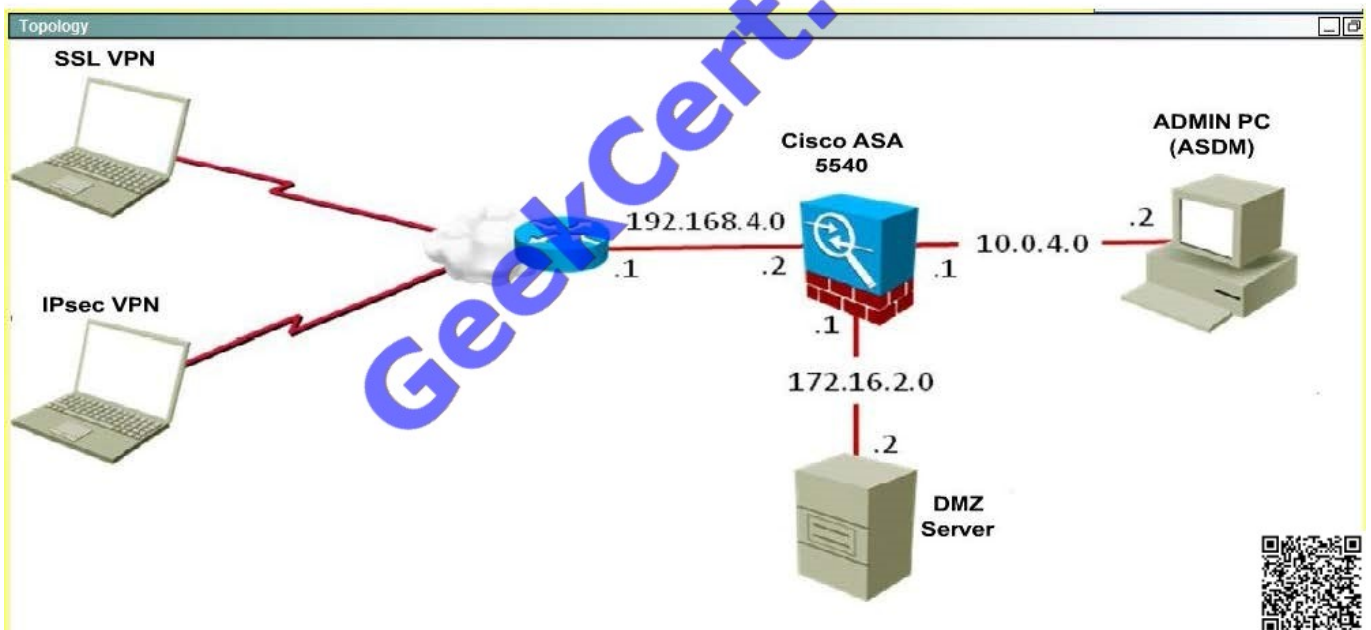
Click the grey buttons at the bottom of this frame to view the different windows.

Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

The "Tab" key and most commands that use the **Control** or **Escape** keys are not supported and are not needed to complete this simulation.

**Scenario**

You are the firewall administrator for a small company. The company currently supports remote-access SSL VPN and IPsec VPN via a Cisco ASA 5520. This morning, your manager supplied you with a list of Cisco ASA configuration questions. Using the Cisco ASA ASDM, your job is to navigate the preconfigured Cisco ASDM to find the answers to the questions.





The screenshot shows the ASDM configuration page for 'AnyConnect Connection Profiles'. The left sidebar shows the configuration tree with 'Remote Access VPN' expanded. The main content area is titled 'Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles'. It contains the following sections:

- Introduction:** The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.
- Access Interfaces:** A checkbox 'Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below' is checked. A note states: 'SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch)'. Below this is a table:

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Login Page Setting:** A checkbox 'Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.' is checked. A checkbox 'Shutdown portal login page.' is unchecked.
- Connection Profiles:** A note states: 'Connection profile (tunnel group) specifies how user is authenticated and other parameters.' Below this are buttons for 'Add', 'Edit', and 'Delete'. A table lists the connection profiles:

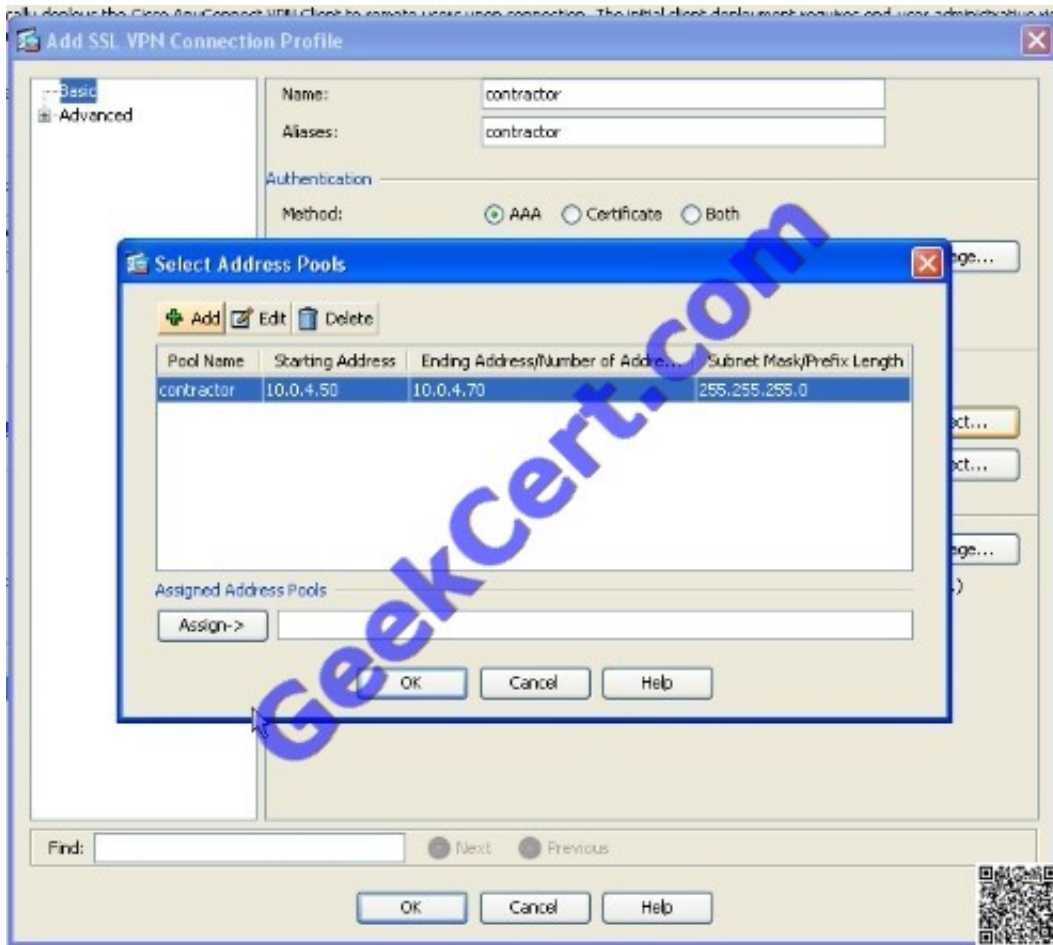
Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method
DefaultRAGroup	<input checked="" type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)
employee	<input checked="" type="checkbox"/>	<input type="checkbox"/>	employee	AAA(LOCAL)

Buttons for 'Device Certificate' and 'Port Settings ..' are visible on the right side of the configuration page.

- A. Is sourced from the contractor pool
- B. Is sourced from the employee pool
- C. Is sourced from the engineering pool
- D. Is sourced from the management pool
- E. Is a dedicated address (10.0.4.1 20)

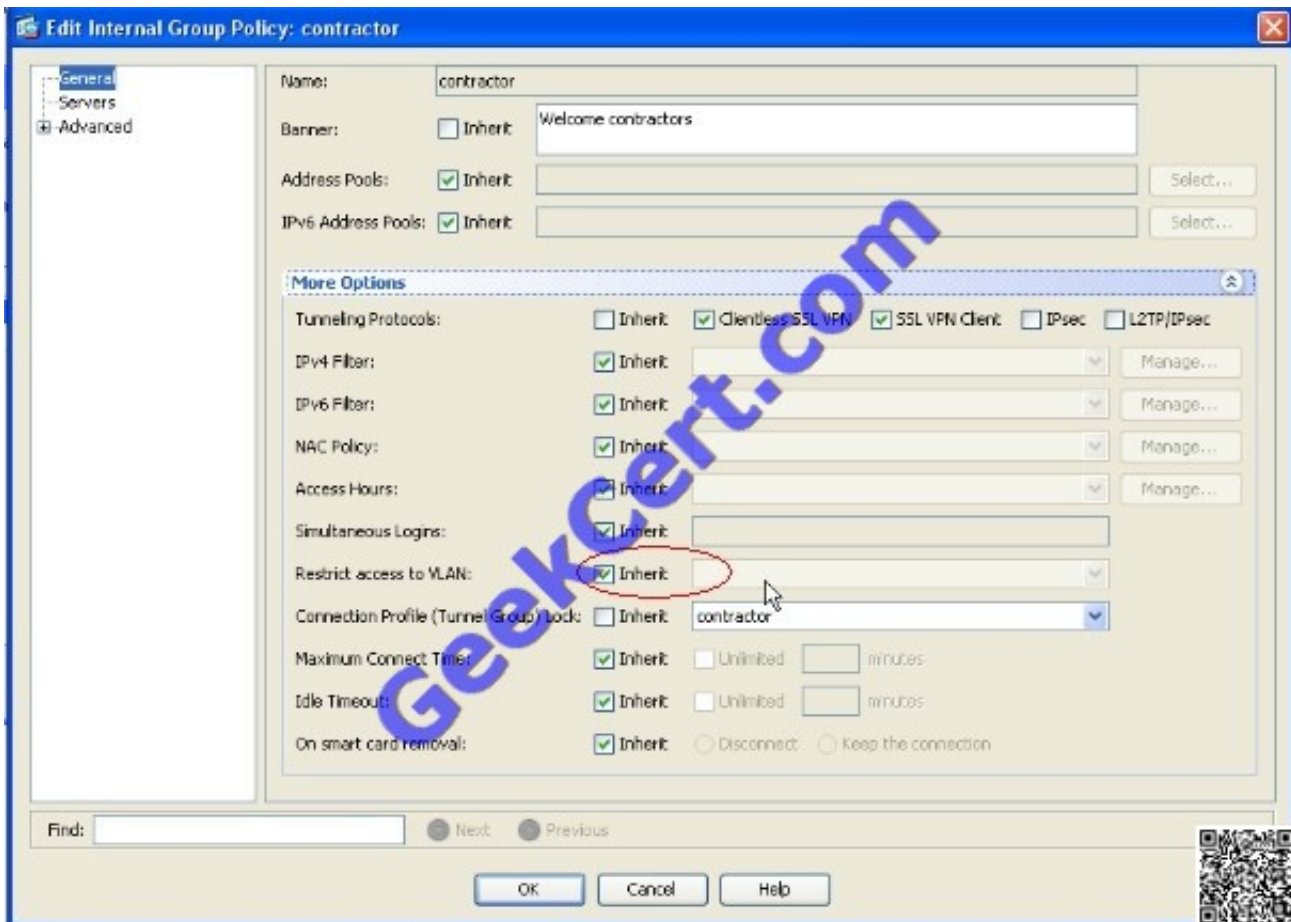
Correct Answer: A

Explanation:



Through configuration first see username in device management >> see its group policy then go to remote access VPN >> connection profiles >> client address pools >> contractor >> select t see the address pool Through Monitoring VPN statistics > session >> see username and its assigned ip address >> then find it out in configuration tab above procedure





### QUESTION 3

Which two statements about the Cisco ASA cluster load-balancing feature are correct? (Choose two.)

- A. The Cisco ASA load-balances both site-to-site and remote-access VPN tunnels.
- B. The Cisco ASA load-balances remote-access VPN tunnels only.
- C. The Cisco ASA load-balances IPsec VPN tunnels only.
- D. The Cisco ASA load-balances IPsec VPN and Cisco AnyConnect SSL VPN tunnels only.
- E. The Cisco ASA load-balances IPsec VPN, clientless, and Cisco AnyConnect SSL VPN tunnels.

Correct Answer: BE

[http://www.cisco.com/en/US/docs/security/asa/asa71/asdm51/selected\\_procedures/asdm\\_lb.html#wp1005](http://www.cisco.com/en/US/docs/security/asa/asa71/asdm51/selected_procedures/asdm_lb.html#wp1005) Eligible Clients Load balancing is effective only on remote sessions initiated with the following clients:

?isco VPN Client (Release 3.0 and later)

?isco VPN 3002 Hardware Client (Release 3.5 or later) ?isco ASA model 5505 when configured as a hardware client ?isco PIX 501/506E when acting as an Easy VPN client. Load balancing works with both IPsec clients and WebVPN

sessions. All other clients, including LAN-to-LAN connections, can connect to a security appliance on which load



balancing is enabled, but they cannot participate in load balancing.

[http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn\\_params.html#wp1048834](http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_params.html#wp1048834)

#### Load Balancing

Load balancing is a mechanism for equitably distributing remote-access VPN traffic among the devices in a virtual cluster. It is based on simple distribution of traffic without taking into account throughput or other factors.

A load-balancing cluster consists of two or more devices, one is the virtual master, and the other devices are the backup. These devices do not need to be of the exact same type, or have identical software versions or configurations.

---

#### QUESTION 4

When troubleshooting a site-to-site IPsec VPN deployment, you see a QM FSM message. What is the most likely cause of this message?

- A. The Quick Mode timers have expired.
- B. There are mismatched proxy identities.
- C. Forward Secrecy Mode has failed.
- D. IKE Phase 1 has failed authentication due to mismatched DH groups.

Correct Answer: B

[http://www.cisco.com/en/US/tech/tk583/tk372/technologies\\_tech\\_note09186a00800949c5.shtml#qms](http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a00800949c5.shtml#qms)

#### QM FSM Error

The IPsec L2L VPN tunnel does not come up on the PIX firewall or ASA, and the QM FSM error message appears. One possible reason is the proxy identities, such as interesting traffic, access control list (ACL) or crypto ACL, do not match on both the ends. Check the configuration on both the devices, and make sure that the crypto ACLs match.

Another possible reason is mismatching of the transform set parameters. Make sure that at both ends, VPN gateways use the same transform set with the exact same parameters.

---

#### QUESTION 5

Refer to following Exhibit and answer the following question below:



### Instructions

Click the grey buttons at the bottom of this frame to view the different windows.

Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

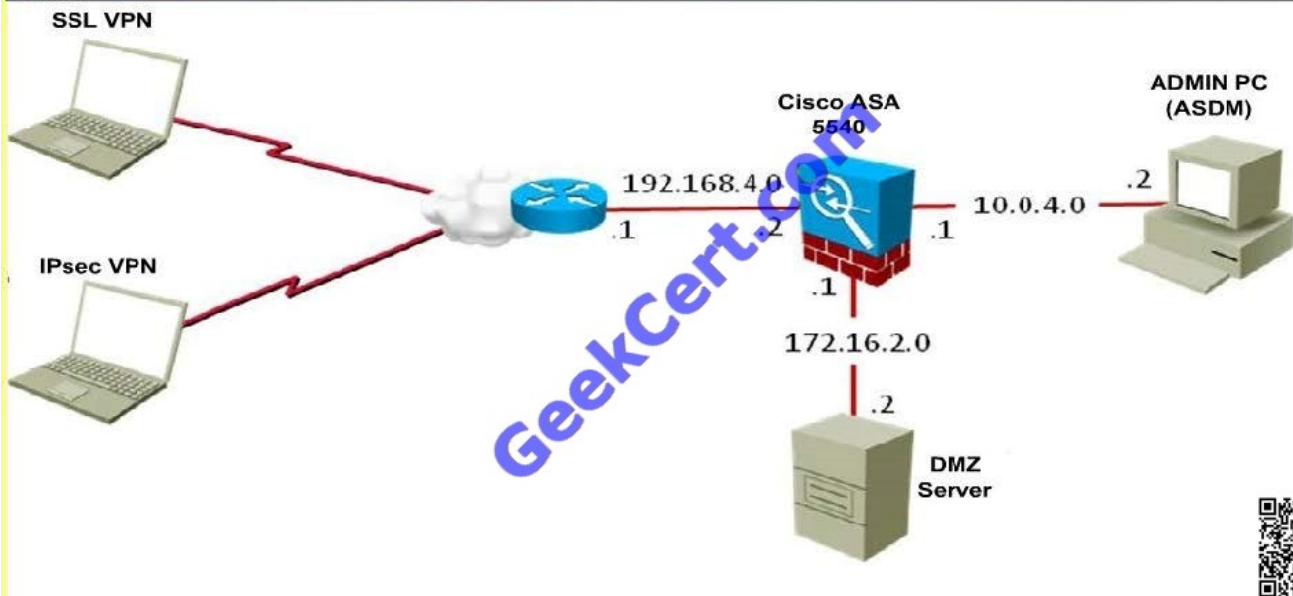
The "Tab" key and most commands that use the **Control** or **Escape** keys are not supported and are not needed to complete this simulation.

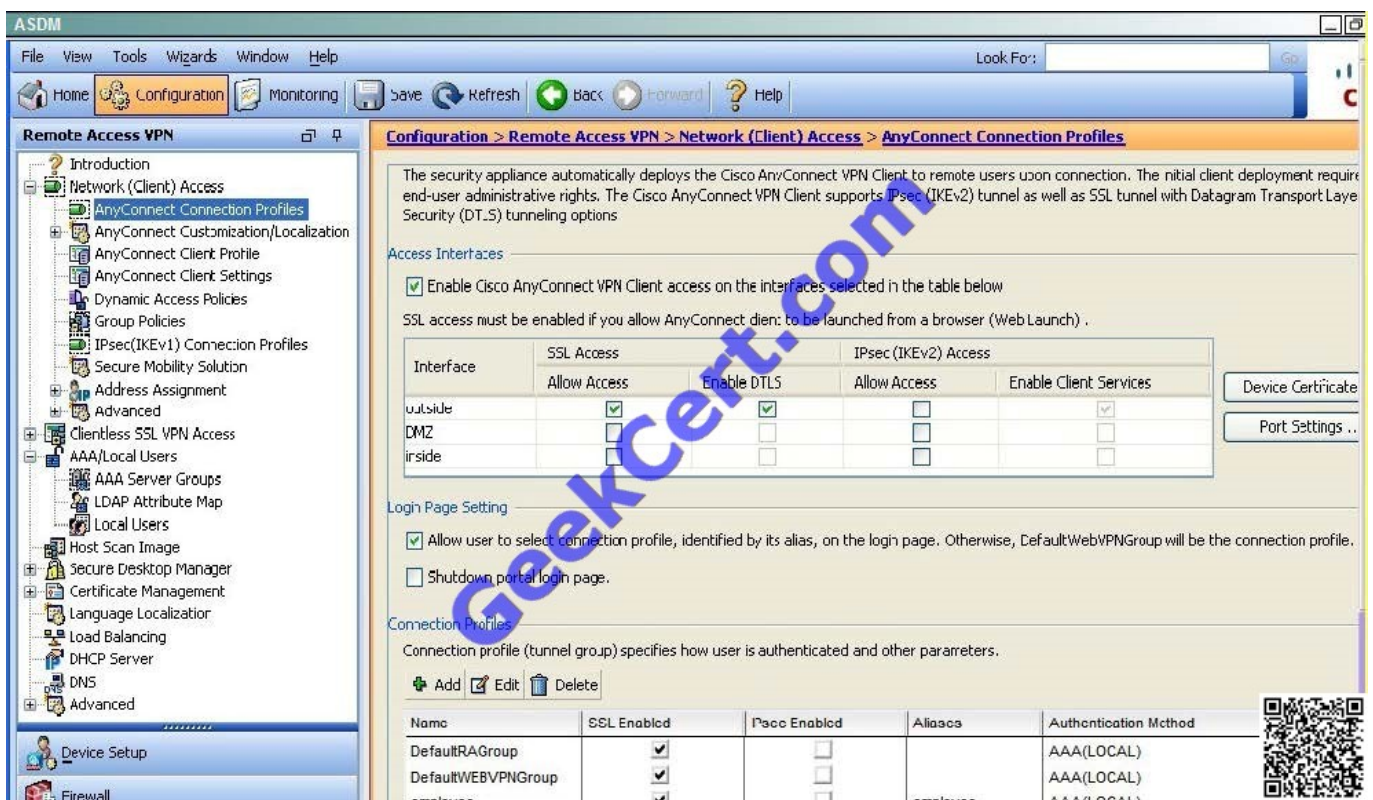
### Scenario

You are the firewall administrator for a small company. The company currently supports remote-access SSL VPN and IPsec VPN via a Cisco ASA 5520. This morning, your manager supplied you with a list of Cisco ASA configuration questions. Using the Cisco ASA ASDM, your job is to navigate the preconfigured Cisco ASDM to find the answers to the questions.



### Topology





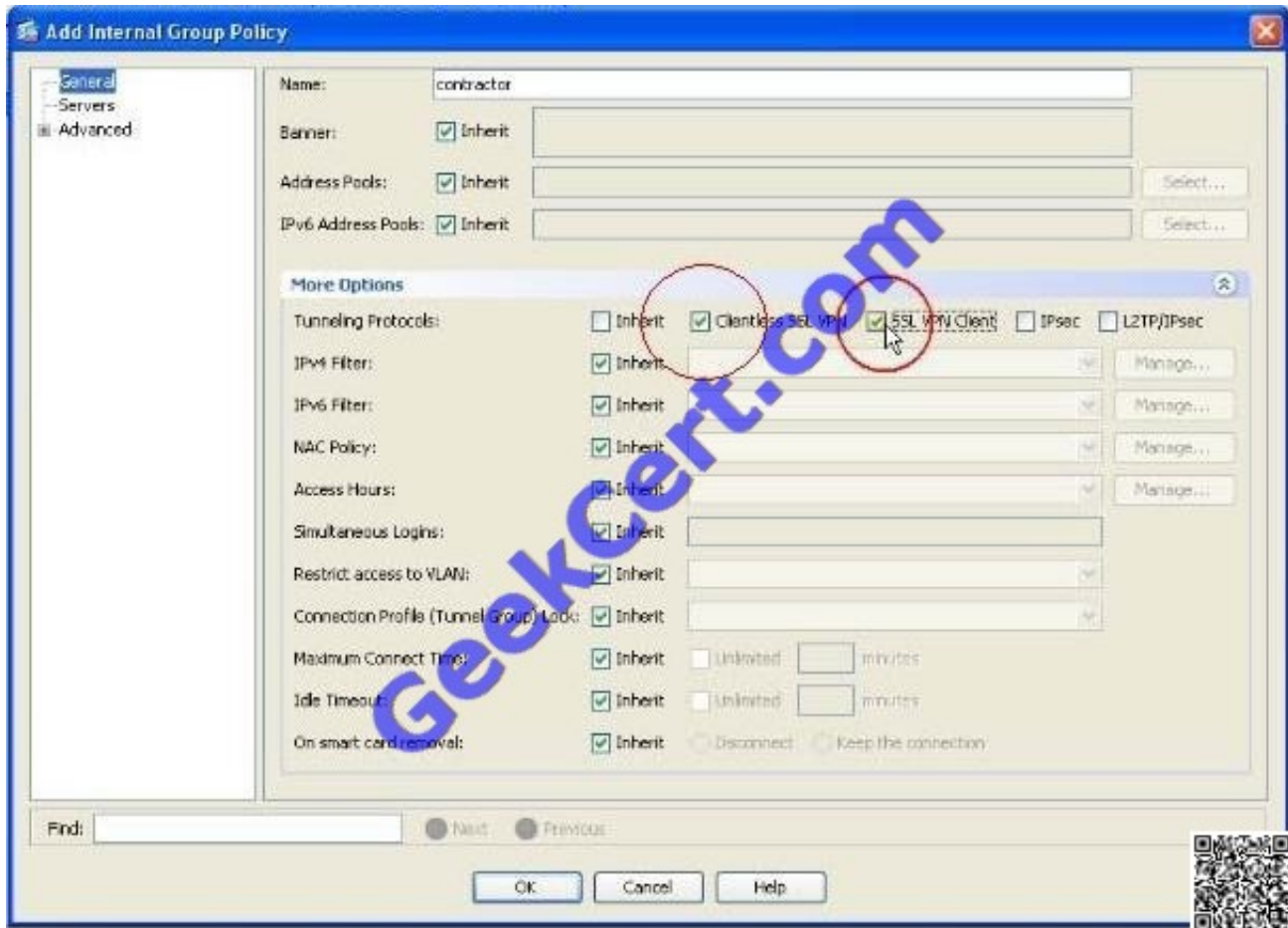
After providing the correct VPN login credentials, user, contractor1, is enabled to use which VPN access type?

- A. Cisco Any Connect VPN
- B. Clientless VPN
- C. Cisco Any Connect VPN and clientless VPN
- D. Cisco Any Connect VPN, clientless VPN, and IPsec VPN

Correct Answer: C

Configuration > network client access > any connect connection profiles > connection profiles > edit for each profile > general > more options > tunneling protocol > see the check marks Monitoring > VPN > VPN statistics > sessions filter by >>> choose contractor1





Monitoring > VPN > VPN statistics > sessions filter by >>> choose contractor1



**Cisco ASDM 6.1 for ASA - Demo mode**

File View Tools Wizards Window Help Look For:  Go

Home Configuration **Monitoring** Save Refresh Back Forward Help

**Device List**

- 10.79.111.254
- localhost:55000

**VPN**

- VPN Statistics
  - Sessions
  - Cluster Loads
  - Crypto Statistics
  - Compression Statistics
  - Encryption Statistics
  - Global IKE/IPsec Statistics
  - NAC Session Summary
  - Protocol Statistics
  - VLAN Mapping Sessions
- Clientless SSL VPN
  - SSO Statistics
- VPN Connection Graphs

**Monitoring > VPN > VPN Statistics > Sessions**

Sessions

IPsec	SSL VPN								
Remote Access	Site-to-Site	Clientless	With Client	Total	E-mail Proxy	VPN Load Balancing	Total	Total Cumulative	

Filter By: Clientless SSL VPN All Sessions Filter

Username	Group Policy	Protocol	Login Time	Bytes Tx	Bytes Rx	Details
IP Address	Connection Profile	Encryption	Duration			Logout

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions -- Logout Sessions

Refresh

Last Updated: 8/9/12

Error in getting/parsing the monitoring data. <admin> 15 3/16/07 11

[Latest 642-648 Dumps](#)

[642-648 VCE Dumps](#)

[642-648 Practice Test](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

## Try our product !

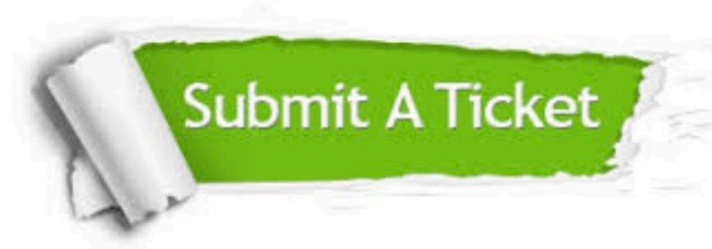
- 100% Guaranteed Success
- 100% Money Back Guarantee
- 365 Days Free Update
- Instant Download After Purchase
- 24x7 Customer Support
- Average 99.9% Success Rate
- More than 800,000 Satisfied Customers Worldwide
- Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.geekcert.com/allproducts>

## Need Help

Please provide as much detail as possible so we can best assist you.  
To update a previously submitted ticket:



 <p><b>One Year Free Update</b> Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p><b>Money Back Guarantee</b> To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p><b>Security &amp; Privacy</b> We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.  
All trademarks are the property of their respective owners.  
Copyright © geekcert, All Rights Reserved.